PTO/SB/33 (07-06)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
8947-000063/US

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

On _____

Signature _____

Typed or printed name _____

Application Number	Filed
10/736,832	December 17, 2003
First Named Inventor: Hee-Kwan SON	
Art Unit: 2193	Examiner: Ngo, C.

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 35,094.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

Signature

John A. Castellano
Typed or printed name

703.668.8000
Telephone number

December 11, 2008
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 forms are submitted.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	10/736,832	Confirmation No.:	5440
Filing Date:	December 17, 2003	Examiner:	Ngo, C.
Applicant:	Hee-Kwan SON	Art Unit:	2193
Title:	MONTGOMERY MODULAR MULTIPLIER AND METHOD THEREOF USING CARRY SAVE ADDITION		
Attorney Docket:	8947-000063/US		

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314
Mail Stop AF

December 11, 2008

ATTACHMENT TO FORM PTO/SB/33
(DETAILS OF PRE-APPEAL BRIEF REQUEST FOR REVIEW)

Sir:

In response to the Office Action ("OA") mailed on October 15, 2007, the Final Office Action ("FOA") mailed on June 11, 2008, and the Advisory Action ("AA") mailed on December 2, 2008, Applicant requests a Pre-Appeal Brief Conference in order to review the claim rejections in the present application. This Details of Pre-Appeal Brief Request for Review is being filed concurrently with a Pre-Appeal Brief Request for Review (Form PTO/SB/33), a Notice of Appeal (Form PTO/SB/31), and a third-month Petition for Extension of Time under 37 C.F.R. § 1.136(a).

Claims 1-61 are pending in the present application. Of these, claims 1, 8, 42, 44, 49, 51, 56, and 61 are written in independent form. Claims 8-41 and 51-55 are rejected[1] and claims 1-7, 42-50, and 56-61 are withdrawn.

[1] The AAF—including proposed amendments to claims 8, 20, 22, 25, 26, and 51—appears to have been entered. Accordingly, claims 8-41 and 51-55 referred to in this document are those claims as listed in the AAF.

REJECTIONS FOR WHICH THE CONFERENCE IS REQUESTED

The panel of the Pre-Appeal Brief Conference ("Panel") is requested to review the rejections of: (1) claims 8-17, 23, 27, and 51-54 under 35 U.S.C. § 103(a) as being unpatentable over "New VLSI Architecture of RSA Public-Key Cryptosystem" by Wang et al. ("Wang"); (2) claims 19-22, 25, and 26 under 35 U.S.C. § 103(a) as being unpatentable over Wang in view of U.S. Patent No. 5,796,645 to Peh et al. ("Peh"); (3) claims 8-41 and 51-55 under 35 U.S.C. § 101; and (4) claims 20 and 22 under 35 U.S.C. § 112, ¶ 2.

Applicant respectfully directs the Panel's attention to the Amendment Under 37 C.F.R. § 1.111 ("Amendment") filed on February 13, 2007, and the Amendment After Final Under 37 C.F.R. § 1.116 ("AAF") filed on November 10, 2008, both of which are incorporated by reference in this paper. Applicant disagrees with the Examiner's rejections of claims 8-41 and 51-55, at least for the reasons given in the Amendment, AAF, and as discussed below.

Applicant's remarks and arguments focus on independent claims 8 and 51. Applicant notes that if claims 8 and 51 are patentable under 35 U.S.C. § 103(a) over Wang in view of Peh, then claims 9-41 and 52-55 also are patentable, for at least the same reasons as claims 8 and 51, from which claims 9-41 and 52-55 directly or indirectly depend.

REMARKS/ARGUMENTS

A. Neither the OA, FOA, Nor the AA Establishes a Proper *Prima Facie* Case of Obviousness for Currently Pending Claim 8 or 51 Over Wang

As discussed in the AAF, Applicant submits that the Examiner failed to establish a proper prima facie case of obviousness for at least the following reasons: (a) assuming, arguendo, that CSA1 includes a plurality of compressors, each of those compressors does not receive at least a multiple modulus q_xN, because the inputs to CSA1 are R_i (or R_{i+2}) and $(2a_{i+1} + a_i)B$;

(b) assuming, arguendo, that CSA2 includes a plurality of compressors, each of those

compressors does not receive at least a partial product a_xB, because the inputs to CSA2 are the partial sum $R_i + (2a_{i+1} + a_i)B$ and $(2q_{i+1} + q_i)N$); (c) neither the input to CSA1 nor the input to CSA2 includes "a corresponding current sum . . . and a corresponding current carry"; (d) neither CSA1 nor CSA2 is "adapted to produce a corresponding next sum and a corresponding next carry"; (e) FIG. 5 of Wang does not disclose "receiving a plurality of . . . corresponding current sums . . . and corresponding current carries to produce a corresponding next sum and next carry"; (f) Wang does not disclose at least "an accumulator including a carry save adder inherently having a plurality of compressors . . . each of the plurality of compressors receiving a multiple modulus (a multiple of N from MUXs), a partial product (a multiple of B from MUXs)"; and (g) Wang does not disclose at least "an accumulator including a carry save adder inherently having a plurality of compressors . . . each of the plurality of compressors receiving . . . a corresponding current sum and a corresponding current carry (the feedback from the [unidentified] carry save adder), and producing a corresponding next sum and a corresponding next carry (the output from the [unidentified] carry save adder)". For at least these reasons, neither the OA, FOA, nor the AA establishes a prima facie case that independent claim 8 or 51 (or any of dependent claims 9-41 and 52-55) is unpatentable over Wang. And for at least these reasons, Applicant requests that the Panel overturn the rejection of claims 8-17, 23, 27, and 51-54 as being unpatentable over Wang under 35 U.S.C. § 103(a).

B. Neither the OA, FOA, Nor the AA Establishes a Proper *Prima Facie* Case of Obviousness for Currently Pending Claim 8 or 51 Over Wang in View of Peh

As also discussed in the AAF, Applicant submits that the Examiner failed to establish a proper prima facie case of obviousness for at least the reasons listed above with respect to Wang and for the following reason: (h) the Examiner does not argue that Peh overcomes the deficiencies of Wang discussed above. For at least these reasons, neither the OA, FOA, nor the

AA establishes a prima facie case that independent claim 8 or 51 (or any of dependent claims 9-41 and 52-55) is unpatentable over Wang in view of Peh. And for at least these reasons, Applicant requests that the Panel overturn the rejection of claims 19-22, 25, and 26 as being unpatentable over Wang in view of Peh under 35 U.S.C. § 103(a).

C. The Amendments to Claims 8 and 51 Obviate the Associated Rejection Under 35 U.S.C. § 101

The AAF amended claim 8 to recite, inter alia, "[a]n accumulator for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier in a cryptosystem" and claim 51 to recite, inter alia, "[a] method of accumulating for accelerating speed of a Montgomery modular multiplier, for reducing power consumption of a Montgomery modular multiplier, or for accelerating the speed of and reducing the power consumption of a Montgomery modular multiplier in a cryptosystem". Applicant submits that independent claims 8 and 51 accomplish a practical application (and, thus, so do dependent claims 9-41 and 52-55); that the practical application yields a real-world result that is useful, tangible, and concrete; that neither the accumulators of claims 8-41 nor the methods of claims 51-55 cover every substantial practical application; and that because the accumulators of claims 8-41 and the methods of claims 51-55 are implemented in associated cryptosystems, they do not preempt use of the underlying algorithm. As a result, Applicant submits that these amendments obviate the rejection of claims 8-41 and 51-55 under 35 U.S.C. § 101.

D. The Amendments to Claims 20 and 22 Obviate the Associated Rejection Under 35 U.S.C. § 112

The AAF amended claim 20 to recite, inter alia, "wherein the compressors of the first group are a first compressor, respectively" and claim 22 to recite, inter alia, "wherein the

compressors of the second group are a second compressor, respectively". Applicant submits that these amendments obviate the rejection of claims 20 and 22 under 35 U.S.C. § 112, ¶ 2.

CONCLUSION

In view of these remarks and arguments, Applicant respectfully requests that the Panel: (1) overturn the rejection of claims 8-17, 23, 27, and 51-54 under 35 U.S.C. § 103(a) as being unpatentable over Wang; (2) overturn the rejection of claims 19-22, 25, and 26 under 35 U.S.C. § 103(a) as being unpatentable over Wang in view of Peh; (3) overturn the rejection of claims 8-41 and 51-55 under 35 U.S.C. § 101; (4) overturn the rejection of claims 20 and 22 under 35 U.S.C. § 112, ¶2; and (5) allow claims 8-41 and 51-55.

Should there be any outstanding matters that need to be resolved in the present application, the Panel is respectfully requested to contact the undersigned at the telephone number listed below.

If necessary, the Director of the U.S. Patent and Trademark Office is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; in particular, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094

P.O. Box 8910
Reston, VA 20195
703.668.8000

JAC/LFG:hcw